

Questions and Answers Regarding Certification and Accreditation of PIV Card Issuing Organizations

Preface: Numerous inquiries have been made to NIST, either directly or through other agencies, regarding achieving the objectives of HSPD-12, satisfying the requirements of FIPS 201, following the instructions of OMB Memorandum M-05-24, and appropriately using the guidelines of NIST SP 800-79. The following set of questions and answers has been prepared to resolve ambiguities that may exist regarding these documents and clarify the precedence of various documents that have been issued and continue to be developed by Federal agencies and their contractors.

HSPD-12 established a new policy regarding establishing the true identity of current and future Federal and contractor employees who use Federal facilities on a regular basis. It required that, within 8 months after the FIPS 201 standard was issued (i.e., by 10/27/2005), “the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard is gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.” HSPD-12 established four control objectives for “secure and reliable identification” of Federal employees and contractors. The control objectives require identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

FIPS 201, Part 1 (PIV-I) “describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12.” Ten requirements are listed in PIV-I stating how and to what extent “each agency’s PIV implementation shall meet the four control objectives.” FIPS 201 then specifies requirements for 1) PIV Identity Proofing and Registration (5 requirements); 2) PIV Issuance and Maintenance (4 requirements); and 3) PIV Privacy (10 requirements). The PIV Identity Proofing and Registration Requirements (FIPS 201 section 2.2) states, “The identity proofing and registration processes used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements 1) and approved in writing by the head of the Federal department or agency.”

NIST Special Publication 800-79 entitled, “Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations” was issued by NIST on its PIV Program website (www.nist.gov/piv-program) on July 27, 2005. These guidelines describe processes and procedures that should be performed in order to satisfy HSPD-12 objective (d) and FIPS 201, PIV-I, PIV Issuance and Maintenance requirement number 5.

OMB Memorandum M-05-24 was issued to all heads of Departments and Agencies on August 5, 2005. “ OMB M-05-25 provides implementing instructions for the Directive

(HSPD-12) and the Standard (FIPS 201).” The answer to question 3 in the Memorandum (“How should I implement Part 1 of the Standard?) includes: “For all new employees, contractors and other applicable individuals, your department or agency must by October 27, 2005, adopt and accredit a registration process consistent with the identity proofing, registration and accreditation requirements in section 2.2 of the Standard Regardless of whether [or not] your agency will be ready to issue standard compliant identity credentials by October 27, 2005.” This registration process will apply to all new identity credentials issued (i.e. no new identity credentials can be issued until these conditions are met).” SP 800-79 is then referenced.

Thus four documents should be consulted, understood, and used while meeting the objectives and requirements involving Federal Personal Identity Verification. HSPD-12 objectives, FIPS 201 requirements (normative sections of the standard), and OMB M-05-24 instructions should be achieved with highest priority. NIST Guidelines such as SP 800-79 should be utilized by the individuals and organizations seeking to implement and use PIV products and services. If a NIST guideline differs from a current FIPS requirement or an OMB instruction, the requirement or instruction should be followed. When other checklists, handbooks, educational materials, white papers, and answers to questions informally provided via the Internet or by telephone provide information that is not consistent with a current FIPS requirement or OMB instruction, the information should be disregarded. However, if the information is consistent and provides improved understanding within a context, then the information should be used as desired but should not be considered as specifying new requirements.

1. What must agencies do before October 27, 2005, to satisfy certification and accreditation (C & A) requirements of PIV-I services?

HSPD-12 requires that any service offered to meet its policy and objectives must assure that an identity credential is issued only by providers whose reliability has been established by an official accreditation process. According to OMB Memorandum M-05-24 dated August 5, 2005, all Federal department and agencies shall satisfy that part of PIV- I specifying PIV Identity Proofing and Registration Requirements and that a certification process will be required to assess the reliability of identity proofing and registration processes. NIST SP 800-79 provides guidelines on how to perform certification assessments of the reliability of a PIV organization and states that an Authorization to Operate should be issued by the Designated Accreditation Authority (DAA) identified by an agency to perform the responsibility of this role before the needed PIV services are provided. Each agency is responsible for accrediting that the processes satisfy the requirements of FIPS 201 Section 2.2.

2. Who is responsible for performing C & A activities?

Each Federal department and agency is responsible for performing C & A of any PIV service before it is used. A Designated Accreditation Authority (DAA) and one or more Certification Agents (CA) should be designated by each agency for

PIV accreditation. These may or may not be the same people as those performing C & A of the security of each agency's computer systems. The roles and authority of the DAA and CA should not be delegated to contractors but the functions supporting CA may be delegated or contracted.

3. What is the process that will have to be followed by a company that wants to become a certified card issuer service provider? Will NIST provide C & A services?

There are no designated organization assigned to address contractor accreditation. Therefore, contractor should follow the same self-accreditation procedure and make the evidence available for the agencies to review by request.

4. What are required and desired attributes for a person or organization doing C & A?

A person or organization performing a PIV organization C & A should exhibit the same attributes specified in SP 800-79 for a PIV organization (i.e., knowledgeable, trustworthy, capable, available, accountable, compliant with standards of quality and good practice, adequately funded and supported with appropriate facilities, equipment, and time). The agencies must ensure the person or organization understands and is an expert on the technical requirements of FIPS 201 and associated special publications.

5. Can a Certification Agent (CA) and an agency's Designated Accreditation Authority (DAA) be within the same organization?

A DAA and a CA may be within the same organization but the CA function should not be within the organization being accredited and the roles should be selected so there is no conflict of interest which impacts or prohibits the independence of the CA function. It should be demonstrated that there exists no conflict of interest across these roles. As an example, the CA should not be involved with the management responsibility for PIV implementation.

6. Should all agencies within a department use the same identity proofing, registration, and issuance process?

It is expected that an agency-wide policy and strategy will be established for identity proofing, registration, and credential issuance. The department may delegate the implementation responsibility to the agencies provided that resulting processes are consistent with the agency-wide policy.

7. Do all agencies have to adhere to one of the approved models in Appendix of FIPS 201?

Agencies are encouraged to use one of the two models. However, the models in FIPS 201 may be viewed as reference models and an agency may decide to modify a model for its use but must demonstrate comparability in terms of roles, functions and required separation of duties. The head of the agency must ensure that the modified and adopted model meets the identity proofing and registration requirements of FIPS 201 to meet PIV-I requirements. For PIV-I, the agency head must approve whichever model is selected or whichever set of processes are certified as meeting the PIV-I requirements.

8. What is reliability? How can the reliability of an organization be certified and accredited?

Factors for assessing the reliability of a PIV organization or service are provided in SP 800-79. These factors include: knowledge of the PIV subject, capability of performing the required PIV tasks, accountability to the agency utilizing the PIV services needed, availability of the PIV organization when and where PIV services are needed, operation of the offered PIV services within a legally structured and operated organization, properly structured and managed PIV organization to ensure continued reliability after initial C & A, trustworthiness of all the people within the organization providing PIV services, adequate resources (facilities, equipment, staff, money, authority) to reliably perform PIV services, and security posture of the facility, equipment, people, and activities of the PIV organization. Other desirable factors include adaptability, cost effectiveness, responsiveness, and cooperativeness should also be considered when assessing the reliability of a PIV organization or the services it offers. SP 800-79 provides guidance on assessing these factors using various methods of assessment. If the assessments result in a recommendation by the CA that the PIV organization is reliable and capable of providing the offered PIV services in accordance with FIPS 201, OMB instructions, and agency policy, then the DAA should issue an authorization to operate as depicted in SP 800-79 Appendix D.

9. I am a part of a small agency which does not have any PIV process in place. Who should I contact regarding providing PIV issuing services?

There is a sponsorship program being made available for small agencies. Small agencies that currently receive human resource and/or financial services from other agencies are encouraged to contact those entities first for assistance. Otherwise, they should contact one of the Sponsoring organizations. As services become available they will be announced on the Federal Identity Credentialing website. (Source: GSA)

10. We have situations where a Registrar would begin the identity proofing process of a job applicant during the application stage by collecting fingerprints and verifying I-9 source documents before the hiring manager officially decides to extend an offer of employment. After an offer is made, the Registrar then completes the process by initiating the NACI or higher background investigation.

The Issuer would not issue an ID card until both Registrar and Sponsor functions are completed. For the role based model, is it a requirement that the Sponsor function must occur before the Registrar?

Agencies are required to define and adopt a model for identity proofing and applicant registration that meets their needs in their environments and that satisfy the objectives of HSPD-12. The order of performing some services is immaterial to satisfying the objectives and requirements of the identity proofing and registration processes. Some services may be partially completed and others initiated. The goal is to obtain a highly reliable set of processes that ensure security, privacy, and accuracy of the PIV processes and results. A complete assessment of requirements versus methods of satisfying should be done before the agency head approves the customized model.

11. If an agency chooses a model different from the two specified in FIPS 201 Appendix A or modifies either one, what is the process to request approval of a new model?

As stated in FIPS 201 section 2.2, “The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements of section 2.2 and approved in writing by the head of the Federal department or agency.” The models used in FIPS 201 Appendix A should be viewed as reference models. The two examples are ones designed to satisfy the requirements so that obtaining agency approval is easy. Any new model or changes from the example models must be analyzed and satisfaction of the requirements must be demonstrated when recommending approval to the department or agency head. An agency head has full authority to accept a modified model deemed to meet FIPS 201 requirements.

12. It may not be feasible to have separate individuals for each role in either of the recommended models but the requirement for the separation of duties can be satisfied. Authorized agency official signatures on PIV forms and audit trail documentation, as well as the training and certification of the individual, can confirm that the separation of duties requirement is met in a manual mode of PIV identity proofing and registration. An individual performing two identity proofing and registration roles would never be a PIV Card/Credential Issuer, thus providing additional checks-and-balances. Can an individual perform both the Registrar and Sponsor role as long as there are signed agreements and processes that preclude the individual from issuing a PIV Card?

Identity proofing and applicant registration may be performed in various ways that satisfy the objectives of HSPD-12 and the requirements of FIPS 201. No individual should be able to perform all the roles and services required to issue a valid PIV card to another person or to his or her self. An agency head must request analysis of the model for these processes to be used by an agency and then

verify that all relevant requirements are satisfied. The model may then be approved for use by that agency.

13. SP 800-79 states that identity source documents must be stored. FIPS 201 specifies that storing the documents is discretionary. Which has precedence?

FIPS 201 requires the storage of specific details regarding the source documents but not necessarily the document itself or a scanned image. FIPS 201 is worded as it is because copying and retention of copies of some I-9 documents (e.g., passports) is prohibited within some organizations. FIPS 201 requires storage of specific details regarding the source documents and not necessarily a scanned image. SP 800-79 storage guidance should be interpreted as specified in FIPS 201.